Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
NAI1P647/02.262.01

I hereby certify that this correspondence is being e-filed with the USPTO	Application Number	Filed
on January 29, 2009	10/674,878	09/29/2003
Signature /Dana Chan/	First Named Inventor: David Currie	
Typed or printed name Dana Chan	Art Unit: 2435	Examiner: Paliwal, Yogesh

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KEVINZILKA/
Signature

Kevin J. Zilka
Typed or printed name

408-971-2573
Telephone number

January 29, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

REMARKS

The Examiner has rejected Claim 42 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. More specifically, the Examiner has argued that they were "unable to find support for this limitation in [the] original disclosure." Applicant respectfully disagrees and respectfully directed the Examiner's attention to Page 15, lines 7-10, which disclose that "the scanning engine is invoked for each device the customer service 102 has registered in the customer information database 304 according the schedule requested for that device" and that "[i]n one example, customers are offered five possible queue times to schedule scans of their service 102" (emphasis added). Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

The Examiner has rejected Claims 1, 2, 9, 21, 27-30, 35, 38-39, and 41-45 under 35 U.S.C. 103(a) as being unpatentable over Khaishgi et al. (U.S. Patent No. 6,658,394), in view of Guirguis ("Network- and Host-Based Vulnerability Assessments: An Introduction to a Cost Effective and Easy to Use Strategy"), further in view of Tiso ("Automated Security Scanning"), and further in view of Bunker, V et al. (U.S. Patent Publication No. 2003/0028803). Applicant respectfully disagrees with such rejection.

With respect to the independent claims, the Examiner has relied on Page 2, second paragraph, and Page 6, Section 3.14 from the Guirguis reference to make a prior art showing of applicant's claimed technique "wherein the scanning produces a set of XML files including information about open ports, available service, network protocols, security exposures and vulnerabilities associated with a device providing the on-line service" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully notes that the above excerpts relied on by the Examiner merely disclose that "professionals can use both network- and host-based vulnerability assessments (VSs) to obtain a complete evaluation of the security risks of the system(s)

under investigation," where vulnerability assessments "point out which systems are noncompliant with the company security policies" in addition to "locat[ing] which systems are vulnerable… identif[ying] what services/components are vulnerable, and… suggest[ing] the best method for repairing the vulnerabilities (i.e. – it recommends which patch or software version should be used/applied)" (Page 2, second paragraph – emphasis added).

Additionally, the excerpts disclose that "Nessus network VA reports… provide a complete overview of the target system's vulnerabilities" and "include a list of open ports detected, services associated with these ports, and vulnerabilities associated with these services along with suggested fixes with related CVE identifications and BID identifications," in addition to disclosing that "[e]ach problem detected by Nessus is categorized into one of four severity levels," where "Nessus categorizes high severity problems as security holes, while medium/low severity problems as warnings and finally informational problems as open ports" (Section 3.1.4, first paragraph – emphasis added). Further, the excerpts disclose that "[t]he assessment results can either be exported into different formats such as NSR, Extended NSR, SQL command File, CSV, ASCII text, HTML, XML, and Adobe PDF files, or stored in a central MySQL database" (Section 3.1.4, second paragraph).

However, merely evaluating security risks of a system by identifying noncompliant systems and vulnerable services or components, where vulnerability assessment reports provide an overview of a system's vulnerabilities and include detected open ports, services associated with the ports, and vulnerabilities associated with the services, as in Guirguis, fails to disclose a technique "wherein the scanning produces a set of XML files including information about open ports, available service, network protocols, security exposures and vulnerabilities associated with a device providing the on-line service" (emphasis added), as claimed by applicant. Merely disclosing a vulnerability assessment report which includes detected open ports, services associated with the ports, and vulnerabilities associated with the services, as in Guirguis, fails to disclose a technique "wherein the scanning produces a set of XML files including…

network protocols... associated with a device providing the on-line service" (emphasis added), as specifically claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 34, the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Khaishgi, in view of Guirguis, in view of Tiso, in view of Bunker, V, and further in view of "Nessus Scan Report" (http://web.archive.org/web/20001217231600/www.nessus.org/demo/report.txt).

Specifically, the Examiner has relied on the following excerpt from the Nessus Scan Report reference to make a prior art showing of applicant's claimed technique "wherein the database stores the information about the open ports on the device providing the online service, generic services expected to be running on the open ports, and actual services running on the open ports, including a version and network message protocol associated with the actual services."

"Information found on port ftp (21/tcp)

bonsai microsoft ftp service (version 4.0).

500 'get / http/1.0': command not understood"

(Nessus Scan Report, "DETAILS")

Applicant respectfully notes that the above excerpt relied on by the Examiner merely discloses information found on a particular port, including a service ("bonsai microsoft ftp service") running on the port and the version of the service. However, merely disclosing a service running on a particular port, as in the Nessus Scan Report reference, fails to disclose a technique "wherein the database stores the information about the open ports on the device providing the online service, generic services expected to be running on the open ports, and actual services running on the open ports, including a version and network message protocol associated with the actual services" (emphasis added), as claimed by applicant. Merely disclosing a service running on a particular port, as in the Nessus Scan Report reference, fails to disclose a technique "wherein the database stores the information about... generic services expected to be running on the open ports" (emphasis added), as specifically claimed by applicant.

Additionally, with respect to Claim 36, the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Khaishgi, in view of Guirguis, in view of Tiso, in view of Bunker, V, and further in view of Blyth ("An XML-based architecture to perform data integration and data unification in vulnerability assessments").

Specifically, the Examiner has relied on Page 16, first paragraph, as well as Figures 1 and 6 (reproduced below) from the Blyth reference to make a prior art showing of applicant's claimed technique "wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with an account number of a provider of the online service."

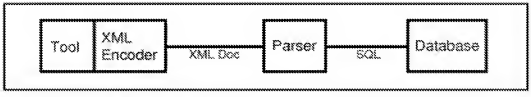

Figure 1: The general architecture.

```
# psxml -p 80 -v -h 10.65.19.12 | xmldb -v -c
/etc/xmldb.conf
The PortScanning XML Tool Version 1.0 (ajcblyth@glam.ac.uk)
Interesting ports on www.my-victim.com (10.65.19.12)
Port            State       Service
80              open        http
Connecting to database xmldb on host db.my-hacker.ac.uk
Inserting information regarding port: 80/open/http
```

Figure 6: Port scanning and database tools output.

Applicant respectfully notes that the above excerpt relied on by the Examiner merely discloses that "[t]he output from the port scanning tool, or the vulnerability scanning tool, is used to create the XML document that is then passed to the parser, which uses it to create a DOM tree," and that "[t]he parser parses the XML documents with reference to their document type definitions (DTD) to check that the XML documents are valid and well formed" (Page 16, first paragraph). Additionally, the figures relied on by the Examiner merely disclose a parser, in addition to disclosing "an example of the psxml and xmldb tools running in verbose mode," where "psxml is a simple port scanning tool" and where an "XML document is… passed to the back-end XML database system called xmldb" (Page 19, second paragraph, not specifically cited).

However, merely using output from a port or vulnerability scanning tool to create an XML document that is parsed to check that the document is valid and well formed, in addition to disclosing a port scanning tool and a back-end database system, as in Blyth, fails to disclose a technique "wherein the scanning engine parses the set of XML files and stores records of the parsed set of XML files in the database in association with an account number of a provider of the online service" (emphasis added), as claimed.